



AUP COMPLIANCE

**Auditing the AUP compliance
by using a non-invasive surveillance solution.**

About Acceptable Use Policy

Today, performing at work without a computer is impossible. Besides using computers for job-related activities, I guess everyone has used it at least once to access various web pages or resources for personal purposes. Yet, managers are looking for solutions to reduce employee browsing and using IT equipments for personal use. Thus they expect higher productivity, reduced costs for consumables, eliminating the risk of Internet threats and attacks, and reduced company liabilities.

Schools, corporations, and other concerns have implemented an Acceptable Use Policy (AUP) that the employees/students should follow. AUP is a set of rules applied by many computer networks which restrict the ways in which the network may be used. Enforcement of AUPs varies with the network.

The purpose of AUP is to outline the acceptable use of computer equipment at a certain entity. These rules are in place to protect the employee and the entity. Inappropriate use exposes the company to risks including virus attacks, compromise of network systems and services, and legal issues.

Acceptable use policies are also integral to the framework of information security policies; it is often common practice to ask new members of an organization to sign an AUP before they are given access to its information systems. For this reason, an AUP must be concise and clear, while at the same time covering the most important points about what users are, and are not, allowed to do with the IT systems of the organization. It should refer users to the more comprehensive security policy where relevant. It should also, and very notably, define what sanctions will be applied if a user breaks the AUP. Compliance with this policy should, as usual, be measured by regular audits.

Auditing the AUP compliance by using a non-invasive surveillance solution.

To motivate employee compliance, companies increasingly are putting teeth in technology policies. Workers have been fired on the grounds of misusing the Internet or for e-mail misuse. When it comes to workplace computer use, employers are primarily concerned about inappropriate Web surfing, with 76% monitoring workers' Website connections, according to the latest AMA/ePolicy study on electronic monitoring and surveillance policies and procedures in the workplace. Fully, 65% of

companies use software to block connections to inappropriate websites. Computer monitoring takes various forms, with 36% of employers tracking content, keystrokes and time spent at the keyboard. Another 50% store and review employees' computer files. Companies also keep an eye on e-mail, with 55% retaining and reviewing messages. Fully 80% inform workers that the company is monitoring content, keystrokes and time spent at the keyboard; 82% let employees know the company stores and reviews computer files; 86% alert employees to e-mail monitoring; and 89% notify employees that their web usage is being tracked.

Concern over litigation and the role electronic evidence plays in lawsuits and regulatory investigations has spurred more employers to implement electronic technology policies. Employers, through the AUP have established policies governing personal e-mail use (84%); personal Internet use (81%); personal instant messenger (IM) use (42%); operation of personal Websites on company time (34%); personal postings on corporate blogs (23%); and operation of personal blogs on company time (20%). Workers' e-mail, IM, blog and Internet content create written business records that are the electronic equivalent of DNA evidence.

The software market can offer many solutions for employee monitoring starting from invasive solutions such as keyloggers that monitor ALL computer activity, to complex non-invasive solutions that can provide statistics and reports on a single employee or an entire department.

Amplusnet has come up with a non invasive solution, Cyclope Employee Surveillance Solution that monitors the activity of employees while using their computers. Furthermore, the application provides the IS officer all the reports necessary in auditing the AUP compliance. Its main features cover:

- **Application used:** all run application will show up, including those not accepted by the AUP as the time of use and the percentage of time as from total working time. It is a good indicator to see the job description of each worker and determine what applications can be used. Consulting the chart it is easy to figure it out whether a game or a productive application has been used. An IT administrator can discover the use of unlicensed application whose use may cause liabilities, or damages to the network; the introduction of malicious programs into the network or server (e.g., viruses, worms,

Trojan horses, e-mail bombs, etc.) is prohibited. Applications such as instant messenger, free/personal emails, P2P applications will be visible in the application reports. Cyclope Employee Surveillance is making an application audit, helping network administrators control applications running on a computer, evaluate if computers are properly used or more computers are needed to a specified location.

- **Users Activity:** Cyclope Employee Surveillance gives information on the employee activity as active or idle, and offers the substantiating the productive time or providing evidence in comparing similar job descriptions.
- **Internet Activity:** Employees tend to spend most of their time browsing on the Internet. Cyclope Employee Surveillance gives accurate statistics on what pages have been accessed and how much time the employee spent using them. This report includes also all accessed web applications. One will note the use of pages not accepted by the AUP.
- **Printing activity:** all printing jobs will be closely monitored, providing information on who is printing what, when and how many pages.
- **Document monitoring:** this feature provides detailed information on the document accessed or created and the time the user spend with it.
-

Privacy and legislation

Cyclope Employee Surveillance is not an invasive solution. Identification is made solely by electronic means and does not collect personal information or intercept any means of electronic communication (monitoring messages as they are transmitted). It clearly monitors what an employee is doing at work as far as job description and IT infrastructure is handled. Before implementing a monitoring solution every manager should make sure that it complies with the local laws. Legislation on employee monitoring varies from country to county. The US law generally allows monitoring of employees provided they have no reasonable expectation of privacy. As a result, if companies have given employees clear notice that they will monitor

public areas and technology resources, employees generally will have no reasonable expectation of privacy and a company can monitor. European countries have individually established laws on this matter, yet a new directive dealing with the issues of consent, medical data, drug and genetic testing, and monitoring and surveillance is due to be issued.

Conclusion

Basically, the compliance audit will target the following aspect monitored by the application:

- internet activity
- abusive use of unlicensed materials
- abusive use of company hardware/peripherals (printers, scanners etc),
-

Cyclope Employee Surveillance through its monitoring and reporting features provides the supporting information in assessing the acceptable use policy compliance.

About Amplusnet

Amplusnet Group is a privately owned group of companies operating in the field of development and marketing of software solution and of outsourcing services. The group operates, an estore containing online anonymity and privacy tools, and cyclope-series.com, a portal containing enterprise monitoring solutions.

Cyclope Series points at providing state of the art monitoring and filtering solutions that provide a detailed image on a company's ICT infrastructure usage. Cyclope Series Solutions supports a high employee control, employee productivity and provides means of identify areas of abuse or malpractice.